Selling IBM STG Systems Software to Business Partners

Power SC Overview
Power Systems Security & Compliance

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

© 2012 IBM Corporation
PowerSC → Security + Compliance designed to protect data centers virtualized with PowerVM enabling Higher Quality Services

**Client Benefits**

- **Simplifies management and measurement of security & compliance**
- **Reduces cost of administrating security & compliance**
- **Improves detection and reporting of security exposures**
- **Reduces time and skills needed for the audit capability to satisfy reporting requirements**
- **Provides “virtualization aware” security extensions**

---

**PowerSC Editions**

- **PowerSC Express**
  - Basic compliance for AIX

- **PowerSC Standard**
  - Security and compliance for virtual & cloud environments

---

**PowerSC Editions**

<table>
<thead>
<tr>
<th>Edition</th>
<th>Express</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security &amp; Compliance Automation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Trusted Logging</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Trusted Boot**</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Trusted Firewall ##</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Trusted Network Connect &amp; Patch Mgmt</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Real Time Compliance</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

---

**PowerSC GBP/core**

<table>
<thead>
<tr>
<th>Edition</th>
<th>Express</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Blade up to 750</td>
<td>£91.75</td>
<td>£111.67</td>
</tr>
<tr>
<td></td>
<td>£15.53</td>
<td>£22.34</td>
</tr>
<tr>
<td>Medium Power 770</td>
<td>£229.38</td>
<td>£281.41</td>
</tr>
<tr>
<td></td>
<td>£39.17</td>
<td>£56.28</td>
</tr>
<tr>
<td>Large Power780 &amp; 795</td>
<td>£458.77</td>
<td>£558.35</td>
</tr>
<tr>
<td></td>
<td>£77.99</td>
<td>£111.67</td>
</tr>
</tbody>
</table>

**UK List prices from mid-2012 = only indicative of a ball-park. Please ask for a current price in your country & currency.**

**“Requires POWER7 System with eFW7.4 Supports IBM i & Power Linux.”**

---

Selling IBM STG Systems Software to Business Partners

---
IBM Power System : Secure Virtualization

Designed to provide a secure virtualized environment and lower overall TCO

- Power Systems Hypervisor has never had a single reported security vulnerability; A perfect security record.† No downtime forced by security patches.
- Software based hypervisors such as VMware (93† security vulnerabilities) have a high number of security concerns.

† US Gov and Mitre tracking of Common Vulnerabilities and Exposures
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=VMware
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=PowerVM

- The Power Systems hypervisor is designed for security and isolation plus performance hence using a hardware based hypervisor & LPARs.
- Only hardware firmware (digitally signed by IBM) can be loaded into the Power Systems hypervisor.
- In addition to its proven security record, Power Systems have all of the functionality and management control required to operate in a public cloud environment:
  - Live partition mobility
  - Proven resource isolation between partitions
  - Power Virtualization including the hypervisor and the Virtual I/O server has been certified for EAL4+ Common Criteria
  - Power Systems Hypervisor has never had a single reported security vulnerability; A perfect security record.
  - No downtime forced by security patches.
- Software based hypervisors such as VMware have a high number of security concerns.

Customer Benefits
- Improved efficiency through consolidation
- Secure sharing of common resources such as processors, I/O and memory
- Reduced IT costs
- Flexibility to instantly respond to workload changes

AIX Security is already excellent

Hands up those that think IT Security is exciting? Typically not many ☺

- But it is absolutely important if it is your bank account, credit card, pension, medical records, personal details …!

Actually AIX has excellent security features you are/should be using already
- ssh / sftp
- RBAC = Roll based Access Control
- Encrypted JFS2 filesystems
- Extended passwords & secondary challenge response additions
- aixpert, ARTEX, IP filters, permissions manager, user check …..
- Provided it is … AIX 6 & 7 and up to date on TL/service pack

No amount of security software can fix users/sysadmin using telnet or ftp?
IBM i - Built-in Security

Security was designed as an integral part of the system
- Virus resistant, object-based architecture
- Integrated security features
- Integrated Cryptography and Key management
- Integrated User Management Interfaces
- Intrusion Detection
- Object based authority
- Native IBM i Audit Journal
- SSL
- VPN
- Encrypted backup
- Encrypted data at rest
- IBM i EAL4+ CAPP certified
- Wealth of ISV applications

No advisories (no security warnings) for IBM i 7.1:
- www.secunia.com → Vulnerability Report: IBM i 7.1 :

Security has issued a total of 9 security advisories in 2003-2013 for IBM i 7.1. Currently, 0 out of 9 are marked as unpatched.

More information about the specific Security advisories affecting IBM i 7.1 can be found below. Each Security advisory is encoded by a box highlighting the current patch table.
You can read the complete Security advisories for thorough descriptions of the issues covered and for security suggestions by clicking either the Security advisory title or the “Read More” link available for each advisory.

PowerSC and IBM i

Supported PowerSC features:
- Work on all operating Systems (AIX / IBM i / Linux):
  - Trusted Firewall✓
  - Trusted Surveyor✓

Some equivalent functionality already in the base IBM i:
- PowerSC Trusted Audit Data Repository → Trusted Logging
  - Very similar to IBM i audit features
  - QAUDJRN (journal & associated journal receivers are read-only objects)
  - cannot be modified by any user
- PowerSC Trusted Digital Signature Verification → Trusted Boot
  - IBM i allows digital signing and verifying of any executables
  - CHKOBJITG command
  - IBM i LIC, OS, LICPGMs are digitally signed by IBM
- IBM i has built-in features to setup/monitor/enforce
  - Password security
  - Authorizations to files/programs/
  - Manage users/system wide security settings
  - ISV solutions for security & compliance provide additional advanced capabilities
- No equivalent IBM i functionality:
  - Trusted Network Connect & Patch Management

More info in the You and i blog entry - PowerSC and IBM i: Integration of Security:
http://ibmsystemsmag.blogs.com/you_and_i/2012/10/powersc-and-ibm-i-integration-of-security.html
PowerSC has Five Components

1 Trusted Boot
   Be sure that boot media & AIX has booted in a known-trusted state

2 Trusted Network Connect
   When an LPAR attempts to join a VLAN, ensure a minimum AIX level

3 Trusted Firewall
   Pass packets securely between LPARs without an external firewall

4 Trusted Logging
   Secure audit files away and safe from malicious modification

5 Compliance Automation
   Raise alerts if any of 100’s of settings of a security policy are violated

Announced late in 2012 two more tools

6. Real-time alerts – no more periodic script running/polling
7. Trusted Surveyor – checks all LPARs on a VLAN + reports changes

---

PowerSC Redbook

Obfuscated name!
Big = 350 pages

Contents:

- Part 1: Business drivers and solution overview
- Part 2: IT security and compliance management business context
- Part 3: Introducing the IBM PowerSC solution
- Part 4: Technical concepts and deployment guidelines
- Part 5: Chapter 3: Security and Compliance Automation
- Part 6: Chapter 4: Real Time Compliance
- Part 7: Chapter 5: Trusted Logging
- Part 8: Chapter 6: Trusted Network Connect and Patch Management
- Part 9: Chapter 7: Trusted Boot
- Part 10: Chapter 8: Trusted Firewall
- Part 11: Chapter 9: Trusted Surveyor
PowerSC – Trusted Boot and Trusted Execution

Overview

Challenge: Ensure that every virtual machine image in your datacenter hasn’t been altered either by accident or maliciously (commonly called a RootKit attack).

PowerSC Solution: Trusted Boot forms the core root of trust for the image, i.e. a foundation for trust. Each stage of the boot process measures the next, starting at the firmware.

Benefits

- PowerSC offers the only solution on the market to form a chain of trust for VMs all the way from boot to OS!
- Improve QoS by reducing the risk of accidental or malicious image tampering
- Reduce the time it takes to ensure that every VM in your datacenter is running authorized and trusted software.

How PowerSC works:
1. Measure the boot process and securely store the results in a Virtual Trusted Platform Module (VTPM)
2. Provide a sealed set of measurements to the requestor
3. Verify these measurements against a reference manifest

Trusted Boot Pre-Requisites

POWER7 C model (or later) for firmware 740-xxx

- AIX 6 TL7 or AIX 7 TL1 (and VIOS 2.2.1.4)

Sorry: no Linux or IBM i

PowerSC documentation page 11-16
While booting the firmware, boot loader & AIX we save details in the VTPM

- Virtual Trusted Platform Module
- OpenPTS extracts the encrypted details
- Software running on an AIX server

Then compared with its saved valued
If the same = Valid
If different = Need escalation

Saved boot details for each VTPM LPAR

Hypervisor with Virtual Trusted Platform Module (VTPM)
Selling IBM STG Systems Software to Business Partners

Setup ssh and Enrol you AIX LPARs

“Enrol” captures current VTPM encrypted settings = Master

List of Trusted hosts = Good

Modified a boot image → it is noticed

Ran bosboot on one LPAR – Can you tell which?
PowerSC – Trusted Network Connect and Patch

How PowerSC works:
• An image that does not meet trusted patch levels will trigger an alert to the administrator
• It is not allowed access to the protected network as it’s a known weakness (missing security enhancements)
• Can automatically update by NIM then allowed

Overview
Challenge: Ensure that images are trusted and at the proper patch level when they connect to the network.
PowerSC Solution: Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately. Offers automated updating of AIX (via NIM)

Benefits
• Reduce business risk by active notification of down level systems via email and SMS.
• Lower admin costs by automatically spotting non compliant systems within the virtual data center and cloud environments
• Lower costs of demonstrating compliance. Monitoring at virtual machine activation proves compliance to patch policy

Trusted Network Connect (TNC) Architecture

All communication uses ssh
TNC Server and Patch Manager can be the same machine

Not all LPARs have to be involved
PowerSC – Trusted Firewall

How PowerSC works:

Provides network isolation and layer 2,3,4 firewalling between workloads

This Firewall will be provided within the VIOS & between Virtual Networks

Overview

Challenge: No LPAR-to-LPAR firewall protection so all network traffic must be routed via an external Firewall and hairpin turn back into the Power System. Customer needs to purchase high bandwidth router based Firewall hardware

Power SC Solution: Provide a VIOS based Firewall managed by VIOS.

Benefits

- Provides network firewall services within the local server virtualization infrastructure to control network traffic between virtual workloads
- Improves performance by providing network firewall services within the server, which does not require an external firewall for VM-to-VM traffic on the same server
- Reduces network resource consumption by eliminating the need to use the external network for VM-to-VM traffic when virtual machines are running on the same server

The Problem

Long route to Firewall & back

Extra Latency

Drives up physical network work traffic
The Trusted Firewall Solution

POWER base machine

Web Server
VM / LPAR

Application Server
VM / LPAR

Database Server
VM / LPAR

Virtual Network

Virtual I/O Server 2.2.1.4
Any supported OS as it is internal to VIOS

Removes Load on
- 2 physical firewall devices
- 4 external links
- 4 hop so reduced latency
- Physical I/O bandwidth use

It is all good, if Trusted Firewall is simple to setup & configure & it is.

Keeping network traffic within the POWER machine

Five stages to get the Firewall configured

1 Install to VIOS disk - smitty installp
2 Load device driver Secure VM - mksvm
3 Start Filtering - vlantfw
4 Define & manipulate filters - genvfilt - lsvfilt - chvfilt - rmvfilt
5 Update rules to Device Driver - mkvfilt
Test Setup:

VIOS controlling the Trusted Firewall

Two LPARs using various comms programs

PowerSC – Trusted Logging

How PowerSC works:
- Trusted Logging provides tamperproof secure centralized protection for AIX audit and system logs and is integrated with PowerVM virtualization
- Limited access to the Secure VM (VIOS) to a few privileged super users
- Guest VM logs can be managed and backed up from a single location within each physical server
- Log scraping agents and reporting agents can be removed from guest OS

Overview

Challenge: Prevent malicious users from “covering their tracks.”

Power SC Solution: Move log events to a secure external VM via the hypervisor. Centralized logging ensures that even when virtual machines are discarded the audit logs remain on the central location for audit purposes.

Benefits

- Discourage malicious activity by ensuring individual accountability; trace actions to authenticated individuals
- Reduce the time it takes to identify tampering and/or unauthorized changes
- Reduce the time it takes to demonstrate Security Compliance by maintaining strict control over audit logs
Trusted Logging Pre-Requisites

Virtual I/O Server 2.2.1.0

- Latest = currently 2.2.1.4 recommended
- AIX 6 TL7+
- AIX 7 TL1+

- With all service packs recommended

Any hardware that runs the above

PowerSC documentation page 22 -24

VIOS Documentation page 144 - 149
http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/topic/p7hb1/p7hb1.pdf

Logging Alternatives

1) Local default AIX Logging

Risks: Your nasty hacker could

- shuts down logging
- removes log
- edits log
- destroys the LPAR and
  we will never work out how/why!

= No post-mortem analysis
3) Commercial products for log management with active use of logs like filter + alert & archive

Trusted Logging Architecture

VSCSI used by
1 Logical Volume from VG Pool
2 whole local disk
3 File-backed from a storage pool
4 SAN LUN
5 SSP LU
6 virtual tape
7 virtual optical

Not NPIV LUN uses vFC
PowerSC Express & Standard Edition

PowerSC – Security Compliance Automation

Overview
Challenge: Demonstrate compliance to Regulatory standards by setting security configurations on systems in a uniform manner.

PowerSC solution: Compare settings across all of the systems in the datacenter against prebuilt profiles, e.g. Payment Card Industry (PCI), DoD STIG and COBIT.

Benefits
- Lower Administration costs by setting security configs in a repeatable manner
- Lower Admin costs by automating compliance reporting
- Automatic remediation of servers that are out of compliance

How PowerSC works:
- A single dashboard monitors compliance and generates audit reports
- Roll out master security setting profiles to all LPARs
- Checks and Reports non-conformance to the prebuilt security profiles – highlighting vulnerabilities or security violation activity

© 2012 IBM Corporation
**AIX Profile Manager Architecture**

**A Systems Director plug-in simple & consistency across multiple systems**

- **Extract** from System A
- **Set** to Systems N
- **Compare**

---

**Security and Performance Profiles**

- XML paragraphs of setting used by 2 AIX commands
  - **ARTEX** is the *performance* settings command
  - **aixpert** is the *security* setting command

Capture the settings from a “reference” machine

Profiles for IT standard requirements supplied with PowerSC Express

You can use these manually on each AIX (man-power intensive)

PowerSC & AIX Profile machine to Systems Director (ISD) allows
  - Mass roll-out of a master set of profiles
  - Via simple ISD user interface or command line
  - Regular checking & reporting of mismatches from the master settings
  - Updating master settings by set, update, capture
Compliance Automation – PCI profile as an example

- Applies to any part of IT that processes, passes or stores credit card information. ([https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/))
- PCI-DSS requirements 70 pages document which describes 12 major security and security configuration sections.
  - Requirement 1: Build and Maintain a Secure Network
  - Requirement 2: Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
  - Requirement 7: Restrict access to cardholder data by business need to know
  - Requirement 8: Assign a unique ID to each person with computer access.
  - Requirement 9: Restrict physical access to cardholder data
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Requirement 11: Regularly test security systems and processes
  - Requirement 12: Maintain a policy that addresses information security for employees and contractors

PowerSC PCI-DSS Coverage
- Approximately 126 XML rules to assist in the configuration in 7 of the 12 requirement areas.

IBM does not promise a profile will guarantee you are conformant – it is a very good start point & could save you man years of effort
A: Home Grown scripts are expensive to maintain and error prone:
   - Who certifies to auditors that these scripts match security standards?
   - Are scripts secure to modification or tampering?
   - What is the cost of maintenance of scripts?
   - Who monitors data security standards and ensures that the scripts are updated?
   - Is there a standard set of scripts in the company or does every group roll their own?
   - What happens when the author of the scripts leave the company?
   - Do all administrators understand what the scripts do and what are the expected results?

   - How fast do you detect some one “fiddling”? 1 day, 1 month, next years audit?

   - If you don’t have two+ people working full-time on security
     then the hackers will overwhelm you as they are 100% full-time.
     So get the IBM security team fighting for you by using their tools.

**Real-Time Compliance (RTC)**

Built in to the AIX Kernel so no polling or cron scripts
As the resource is changed the AIX kernel immediately takes action
Actions are Email or SNMP trap
Built around a AIX Autonomic Health Advisor File System (AHAFS1)
Real-Time Compliance (RTC)

Pre-req: AIX 6 TL7+ and AIX 7 TL1+
Install PowerSC Express
   - powerscExp.rtc & powerscExp.license
Configure with: smitty RTC
   - To set a email server and address
It is an AIX subsystem:
   - lssrc -s rtcd
   - stopsrc -s rtcd
   - startsrc -s rtcd

Config file of pre-defined monitoring is in /etc/security/rtc/rtcd_policy.conf
   - Edit this and start stop or use the chsec command

Problems also go in to the syslogd (if you have it switched on)

Trusted Surveyor

Separate LPP and cost
- You get different media & look for package: powersc.ts
Installed on AIX via installp
- Then you create a users and roles
It runs a web server
- All access is then via a web browser: Firefox 14+ IE8+
Trusted Surveyor

- Probes to get information from HMC, IVM, … etc.
- Snapshots to get the data
- Reports of VM & VLANS in text or CSV

PowerSC Reduces the Cost and Complexity
Trusted Boot and Trusted Execution

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(25min</td>
<td>&lt; 2min</td>
</tr>
<tr>
<td>Time per VM with manual process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual process run/5month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculates</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$166</td>
<td>X 500</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assumptions:
- Before: Maintain a hash list of all trusted executables list 8 hours per year. Includes 25 min to login, compare trusted hash list to system install list, monitor results and remediate a percentage of the systems.
- After: Run Attestation from central console on anyone particular system or all systems

Pocket the savings while you enjoy these additional PowerSC Advantages:
- Improved Systems performance compared with “Known Bad” model scans like Symantec antivirus that slow your systems to a crawl.
- Reduced business risk with real time trusted execution compliance checks
PowerSC Reduces Cost and Complexity

**Trusted Network Connect**

**Before**

- 20 min x 52 x 500 = 520,000 min
- Time per VM to manually confirm SW level and install patch
- Weekly scans
- VMs per Datacenter
- Total Time

**After**

- 480 min
- 519.520
- 361
- $311,712
- Total Time Savings (mins)
- Total Time Savings days
- Total Datacenter Savings per Year
- Automatic monitoring with minor policy maintenance

Pocket the savings while you enjoy these additional PowerSC Advantages:
- Actively detect compliance vulnerabilities
- Reduce your business risk from VMs that were paused or shutdown during a maintenance update and then restarted and joined the network with unpatched vulnerabilities.

---

**PowerSC Reduces Cost and Complexity**

**Security Compliance Automation**

**Before**

- (150 min - 10 min) x 12 = 1,680 min
- Time per VM to review/limit/accept Security settings
- Time per VM with PowerSC without security
- Weekly scans
- Monthly scans
- Time saving/period
- VMs per Datacenter
- Total Datacenter Savings

**After**

- $1,008 x 500
- 683 days
- $604,000
- Total Datacenter Savings per Year

**Assumptions:**
- Before: manual process of setting or monitoring dozens of compliance configuration settings or maintaining home grown scripts, error prone.
- After: completely automated showing exceptions

**Pocket the savings while you enjoy these additional PowerSC Advantages:**
- Smile when there’s an audit! Count on PowerSC to produce your compliance report for every image in the AIX datacenter in under 10 mins.
- Use PowerSC templates to reduce errors in interpreting and applying complex regulatory standards like PCI, DoD STIG, and COBIT.
Selling IBM STG Systems Software to Business Partners

Learn more about PowerSC on the Web
http://www.ibm.com/systems/power/software/security/

IBM PowerSC
Meeting needs for IT security compliance

Overview Features & benefits Solutions Platform offerings Resources

Power is security and compliance. IBM PowerSC™ provides a security and compliance solution optimized for virtualized environments on Power Systems™ servers, running PowerVM™ and AIX®. Security control and compliance are some of the key components needed to defend the virtualized data center and cloud infrastructure against ever evolving new threats. IBM’s business-driven approach to enterprise security used in conjunction with solutions like PowerSC make IBM the premier security vendor in the market today.

Highlights
- Simplify security management and compliance measurement
- Reduce administration costs of meeting compliance regulations
- Ensure virtualized environments meet same security levels as physical servers
- Improve the audit capabilities for virtualized systems
- Reduce time and skills required for preparation of security audits
- Improve detection of security exposures in virtualized environments

Learn more
- IBM PowerSC data sheet (US/CA)
- IBM security
- IBM Security markets
- IBM Security Reader

Browse Power Systems
- Hardware
- Solutions
- Operating systems
- Migration to Power
- System software
- IBM Security
- Community
- Support & services
- Success stories
- Resources
- News
- Education

Are you Vulnerable?
- Try a complimentary Security Health Scan to
  - Take a holistic approach at business-driven security (US/CA)

IBM DeveloperWorks PowerSC Hands-On Wiki Page

- or - -
http://tinyurl.com/newAIXwiki
and take the PowerSC link

http://youtube.com/user/nigelgriffiths
Videos on
- Trusted Boot
- Trusted Logging
- Trusted Firewall (short-cut)
  for AIX aixpert and fpm

What more Information?
• PowerSC Redbook
Selling IBM STG Systems Software to Business Partners